

SPAM POLICY

1. WHAT IS SPAM

The term "Spam" generally refers to unsolicited junk email sent to large numbers of people to promote products or services. However, in Australia the Spam Act has widened the definition of Spam. For example, email that does not clearly identify the sender or does not contain an unsubscribe facility is also considered Spam, regardless of whether it was solicited or not.

Spam email, responsible for around 50% of all Internet transmitted email across the world, is a growing problem for business and home Internet users alike. Billions of emails containing rogue advertisements, offensive content and unwanted promotions are transferred at random into people's private email boxes every day.

2. WHAT ARE THE LAWS RELATING TO SPAM

The Spam Act 2003 and the Spam Code of Practice 2005

The Internet Industry Association's Spam Code of Practice 2005 (the Spam Code) was developed in support of the Spam Act 2003. The Spam code sets out obligations for both ISPs and all Internet users, as well as establishing processes for Internet users to report incidences of Spam and make Spam-related complaints.

The Code obligations, which came into force on 16 July 2006, are enforced by the Australian Communications and Media Authority (ACMA). See the ACMA Spam Information Page for further information on how the ACMA deals with Spam issues.

3. HOW DOES THE CODE DEFINE SPAM

It is important to note that "Spam" as defined by the Spam Code does not merely refer to unsolicited email. Even if a recipient did consent to receiving an email (for example signing up to a mailing list), the email could still be considered Spam if it does not:

- clearly identify the person or entity that authorised it;
- give accurate information on how to contact them; and
- contain an unsubscribe facility.

4. HOW DOES THE SPAM CODE AFFECT ME

All Internet users are obliged to comply with both the Spam Act and the Spam Code and must not otherwise engage in practices that would result in a breach of the Act. Internet users who disregard the code will also be breaching their Acceptable Use Policy and may have their email account suspended or terminated by their ISP.

5. HOW CAN HYPERNET PROTECT AGAINST SPAM

Hypernet filters all email entering the Hypernet network based on the reputation of the source of the email. 'Reputation-based' filtering examines the source IP address of the sender, determines the likelihood that it is Spam and then either accepts or rejects the message.

It is important to note that default filtering may produce some false positives. On the one hand default filtering is necessary to keep the network clear of Spam and viruses and in this way benefits all customers. On the other hand, reputation-based filtering is a complex process and in some cases the filter may prevent legitimate email reaching your mailbox.

Hypernet has also implemented filters on its routers that prevent its customers from being able to directly reach any mail server other than its own. This prevents compromised computers and open proxies from being used to relay Spam.

6. ACCEPTABLE USAGE POLICY

Hypernet maintains a strict Anti-Spam policy and customers who send Spam face suspension and possible termination of their account.

Customers who are suspected of sending Spam and/or are the subject of a Spam Report or Complaint will be warned that they are in breach of their Acceptable Use Policy (AUP). Repeat offenders or Customers who fail to resolve issues with a compromised computer after they have been warned will have their account suspended pending further investigation.

Customers who are responsible for sending Spam themselves are immediately terminated and referred to the Australian Communications and Media Authority who may take action against the spammer to enforce the Spam Act 2003.

A copy of Hypernet's Acceptable Use Policy can be found on our Important Information page on our website.

7. WHAT OTHER METHODS CAN I USE TO PROTECT MYSELF

There are many things you can do both to protect yourself against Spam and to fight the Spam problem in general.

- a. Firstly, ensure your computer is not directly reachable from the Internet, this can be achieved by using a firewall, or a NAT (Network Address Translation) Router (most common broadband modem/routers do this)
- b. Don't sign up for mailing lists or record your email on registration forms, etc unless absolutely necessary. One way spammers can find your email address is by buying email addresses from a list-broker.
- c. Ensure that you read any email from a source that is not 100% trusted in plain text only, and that you do not open attachments from unknown sources. Spammers can detect when you are reading Spam emails by remote html parsing so, if you do not know the person who sent you the email, do not open it and delete it immediately.
- d. Use other filter products

8. HOW CAN I FIGHT BACK AGAINST SPAM

Reporting Spam is the most effective way you can help fight the Spam problem.

If you are receiving Spam email you can report the Spam to Hypernet, the relevant ISP and/or an anti-Spam organisation.

9. HOW TO REPORT SPAM TO HYPERNET

If the Spam you have received comes from a Hypernet host or client, indicated by the IP address in the received header, you can report this to Hypernet by sending an email to abuse@hypernet.com.au with the details about the spam email.

The Spam Code provides that any email user can Report to Hypernet:

Spam originating from the Hypernet network; OR

Spam-related breaches of a Hypernet customer's AUP

Report Spam to Hypernet: abuse@hypernet.com.au using the subject line SPAM REPORT

10. HOW TO REPORT SPAM TO ANOTHER ISP

If your report is regarding Spam that does not originate within Hypernet's network, Hypernet is unable to take any disciplinary action.

If you would like to report Spam received from an address that is not a Hypernet address, we recommend you report this directly to the relevant ISP from which the message originated. Most ISPs maintain a standard "abuse@" address, similar to the Hypernet one listed above, that can be used to report Spam.

11. REPORT SPAM TO AN ANTI-SPAM ORGANISATION

One of the best-known and effective automated Spam reporting systems is SpamCop.

To report to SpamCop you can log onto <http://www.spamcop.net> and follow the instructions there.

The ACMA also have a Spam reporting system, see <http://spam.acma.gov.au> for more information.

12. MAKE A SPAM COMPLAINT TO HYPERNET

If you are a Hypernet customer you are also entitled to make a Spam Complaint under Part 7 of the Spam Code.

Spam Complaints are more serious than Spam Reports and require additional customer information to be processed. The Spam Complaint procedure allows for escalation of unresolved complaints and Spam Reports by Hypernet customers that are unresolved can also be escalated to Spam Complaints upon request.

Further information on our Complaints procedures can be found in the Hypernet Customer Service Charter. Hypernet endeavours to acknowledge all online complaints within 1 hour and to resolve all complaints within 5 working days. If your complaint is more complex we may require more time to investigate. For complex complaints we endeavour to complete all investigations and provide you with a full response to your complaint within 30 calendar days.

Make a Spam Complaint: abuse@hypernet.com.au using the subject line SPAM COMPLAINT

If Spam contains offensive content: the ACMA.

If Spam breaches privacy law: the Privacy Commissioner.

If Spam is misleading and deceptive or otherwise breaches the Trade Practices Act: the ACCC.

Additional information and filters can be found at the following sites:

Internet Industry sites

<http://www.acma.gov.au>

<http://www.iaa.net.au>

Independent sites

<http://www.spammatters.com>

<http://www.spamcop.net>

<http://www.mozilla.org>

<http://www.cauce.org>

<http://spam.abuse.net>

13. HOW DO SPAMMERS FIND MY EMAIL ADDRESS

Spammers can find your address in a number of ways. They can use email generators that make large amounts of random email address. They can buy your email address from a list-broker, and they can also detect when you are reading Spam emails by remote html parsing.

Note: Hypernet does not under any circumstances sell lists of its customers' email addresses.

14. HOW DO I TELL WHERE A SPAM MESSAGE HAS COME FROM

You can only identify the origin of a Spam message through the first Received header of the message. Most email clients hide this information but it can generally be retrieved through advanced options.

See the guides section for how to retrieve the full headers using your mail client by following the links in the menu to the left of this page.

Note that the 'From' address does not indicate the origin of the Spam. A spammer can put anything they like in the 'From' field, and this will usually be the address of a third party innocent victim.

15. I RECEIVE EMAILS SAYING THAT I HAVE SENT SPAM

There are a number of email scams that tell you that you have sent Spam, or that your account has been suspended for spamming.

Whilst the Hypernet Network Abuse Team does send legitimate Spam/virus notification emails to Hypernet customers, these emails do not ask you to click a link, or follow any attachment, and they include the exact date/time the Spam email that triggered it was sent and the IP address it was sent from, as well as any available evidence.

These emails are only to warn you that you may have a virus infection. You should use your own virus scanner, or one of the ones mentioned in the email to scan your computer and remove the Virus.

If you are unable to remove the virus from your PC you may need to have a professional repair your computer.

Note that Hypernet is obliged by Australian Law to terminate your service if your computer continues to send Spam.